REMARKS

This reply is responsive to the Office Action dated February 17, 2006. The specification has been amended to include a cross-reference to related applications. The title has also been changed to more clearly describe the claimed invention. No new matter has been added by these amendments. Claims 52-67, which were previously withdrawn, have been canceled. Claims 1-39 were previously canceled. Thus, claims 40-51 and 68-79 are again presented for the Examiner's consideration in view of the following remarks.

As an initial matter, applicants note that the Office Action Summary on page 2 of the Office Action does not acknowledge whether the drawings are acceptable to the Examiner. Applicants respectfully request that the next communication indicate whether the drawings have been accepted.

The title of the application was objected to as not being descriptive of the claimed invention. A new title has been submitted herewith. Thus, applicants respectfully request that the objection to the title be withdrawn.

Claims 40-51 and 68-79 have been rejected under 35 U.S.C. § 102(b) as being anticipated by Japanese patent publication JP11-187013 ("*Maruyama*"). Applicants respectfully traverse the rejection.

Independent claims 40, 68 and 73 each require "a tag...including position discrimination data that associates each of the encrypted keys with nodes and leaves of a hierarchical tree structure." Examples of a tag and position discrimination data may be found, by way of example only, in paragraph 0119 of the substitute specification, which was filed on January 16, 2003 and is reproduced below:

> **[0119]** Tag part 607 is a tag for indicating a positional relationship of encrypted node keys and leaf keys stored in the data part. An

> attaching rule of this tag will be described with reference to FIGS. 7A to 7C. FIGS. 7A to 7C show an example for sending the enabling key block (EKB) described previously in FIG. 4A as data. The data at that time is as shown in FIG. 7B. An address of a top node included in an encrypted key at that time is used as a top node address. In this case, since a renewal key of a root key K(t)R is included, a top node address is KR. At this time, for example, data Enc(K(t)0, K(t)R) in the uppermost stage is at a position shown in the hierarchical tree shown in FIG. 7A. (The next data is Enc(K(t)00, K(t)0), which is at a position under on the left hand of the previous data in the tree. Where data exists, a tag is set to 0, and where data does not exist, a tag is set to 1. The tag is set as (left (L) tag, right (R) tag). Here, since data exists at the left of the data at the top stage Enc(K(t)0, K(t)R), L tag = 0, and since data does not exist to the right, R tag = 1. Tags are set to all the data to constitute a row of data and a row of tags as, shown in FIG. 7C.

The tag and its position discrimination data are different from an index. See, for example, paragraphs 0109-0121 of the substitute specification. "The index in the EKB of FIG. 4A shows the absolute address of a node key and a leaf key used as a decryption key." (Substitute specification, paragraph 0111.) Furthermore, as stated in the substitute specification at paragraphs 0120-0121:

> **[0120]** The tag is set in order to show at which position of the tree structure data Enc(Kxxx, Kyyy) is positioned. Since the key data Enc(Kxxx, Kyyy) ... are mere enumerated data of simply encrypted keys, a position on the tree of an encrypted key stored as data can be discriminated by the aforementioned tag. Alternatively, for example, data as shown below can be provided using the node index placed in correspondence to the encrypted data as shown in FIGS. 4A and 4B previously without using the aforementioned tag:
>
> 1. 0: Enc(K(t)0, K(t)root)

> 2. 00: Enc(K(t)00, K(t)0)
> 3. 000: Enc(K(t)000, K(t)00)
> 4. ...
>
> **[0121]** However, using such an index as shown above results in a larger size EKB, which is not preferable in distribution through a network. On the other hand, use of the aforementioned tag as index data allows discrimination of a key position using less data.

The Office Action asserts that *Maruyama* discloses the tag and position discrimination data limitations and refers to pages 13 and 14 of the *Maruyama* translation to support its contention. Applicants respectfully disagree.

What the cited portions of the *Maruyama* translation actually state is:

> In order to solve the above-mentioned problem, it forms multiple keys as many as the receiving parties or more first, it arranges multiple keys hierarchical in the form of a tree structure. Next it forms as a key list which has the key arranged hierarchical in multiple receiving parties at the form of a tree structure, and the key which reaches the position of a from the root of the tree structure with this receiving party of a tree structure in each encryption key of a matching and a receiving party.
> (*Maruyama* translation, pg. 13, ll. 1-11.)

> The block diagram of the encryption key production system of this invention is shown in FIG. 6. Block 610 forms multiple keys of the number of receiving party or more first. Next, with block 620, it arranges multiple keys hierarchical in the form of a tree structure. Finally it sets to block 630, it forms as a key list which has the key arranged hierarchical in multiple receiving parties at the form of a tree structure, and the key which reaches the position of a from the root of the tree structure with this receiving party of a tree structure in each encryption key of a matching and a receiving party.
> (*Maruyama* translation, pg. 14, ¶ 0010.)

As can be seen from the above portions of *Maruyama*, the key list has nothing to do with tag and position discrimination data. For instance, there does not appear to be any association of each of the encrypted keys with nodes and leaves of a hierarchical tree structure as claimed. Thus, for at least these reasons, *Maruyama* does not anticipate independent claims 40, 68 and 73. Applicants respectfully submit that the independent claims are in condition for allowance.

Claims 41-51, 69-72 and 74-79 depend from independent claims 40, 68 and 73, respectively, and contain all the limitations thereof. Accordingly, applicants submit that, for at least this reason, the subject dependent claims are likewise patentable.

As it is believed that all of the rejections set forth in the Office Action have been fully met, favorable reconsideration and allowance are earnestly solicited.

If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that he telephone applicants' attorney at (908) 654-5000 in order to overcome any additional objections which he might have. If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: April 27, 2006

Respectfully submitted,

By

Andrew T. Zidel
Registration No.: 45,256
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorney for Applicant